(REDACTED)

FILED UNDER SEAL

EXHIBIT 2

United States District Court
Northern District of California

Case No. 3:22-cv-07465-CRB

Valerie Torres and Rhonda Hyman v. Prudential Financial, Inc., ActiveProspect, Inc., and Assurance IQ, LLC

Expert Report of Zubair Shafiq
in Support of Class Certification

June 28, 2024

PROVISIONALLY FILED UNDER SEAL
(Redacted Version)

I. QUALIFICATIONS

1. I am an associate professor of computer science at the University of California-Davis, where I run a research lab focused on Internet privacy, security, and safety. My lab's research over the last several years has specifically aimed to uncover personal data collection, sharing, and usage in the online advertising ecosystem.

2. In addition to my research, I regularly teach undergraduate and graduate courses on computer networks and computer security, including special topics courses covering emerging trends in online advertising and tracking.

3. I have received several awards and distinctions for my research. I am a recipient of the Chancellor's Fellowship (2022-2023), Dean's Scholar Award (2020), National Science Foundation CAREER Award (2018), and Fitch-Beach Outstanding Graduate Research Award (2013).

4. I have co-authored more than 100 peer-reviewed research papers. I received the Best Paper Award at the 2023 ACM Internet Measurement Conference for my research on tracking, profiling, and ad targeting in the Amazon Alexa ecosystem. I also received the 2018 Andreas Pfitzmann Award at the Privacy Enhancing Technologies Symposium for my research on designing a system to reliably detect advertising and tracking information flows in mobile apps. I also received the Best Paper Award at the 2017 ACM Internet Measurement Conference for my research on identifying and investigating the abuse of a security vulnerability in Facebook Graph API. I also received the Best Paper Award at the 2012 IEEE International Conference on Network Protocols for my research on reverse-engineering proprietary network traffic protocols.

5. I am the editor-in-chief of the Proceedings on Privacy Enhancing Technologies (PoPETs). I am on the steering committee of the Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb). I am the general chair of the Workshop on Technology and Consumer Protection (ConPro). Recently, I have served as the program chair for the Workshop on Technology and Consumer Protection (ConPro 2022 and 2023) and the Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb 2022 and 2023).

6. My full qualifications are set forth in my curriculum vitae, which is attached as Appendix A. The curriculum vitae includes the list of cases in which I have submitted a report, or I have testified at trial or by deposition in the past four years. It also includes a list of publications I have authored in the past ten years.

7. I have been retained by Girard Sharp LLP as an expert in this case. I understand that Plaintiffs allege that ActiveProspect intercepted personally identifiable and sensitive information of natural persons who, while in California, visited Prudential.com, provided personal information on Prudential's form to receive a quote for life insurance, and for whom a TrustedForm Certificate URL associated with that website visit was generated from November 23, 2021 to December 13, 2022.

8. I am being compensated at the rate of $500 per hour for my time. My compensation is not dependent on my conclusions or on the outcome of this action.

9. Appendix B lists the documents that I have considered and relied upon in preparing this report.

10. I reserve the right to amend, modify, or supplement my opinions as new or additional information becomes available to me in advance of trial.

II.   ASSIGNMENTS

11. I was asked by the Counsel for Plaintiffs to analyze the following:

   a. Whether Prudential and Assurance IQ programmed ActiveProspect's source code on Prudential's website to intercept data submitted by Prudential website visitors and send it to ActiveProspect.

   b. Whether data in possession of Prudential, Assurance IQ, and ActiveProspect can be used to identify natural persons whose data was intercepted by ActiveProspect when they filled out a webform to request a life insurance quote on Prudential's website.

III.   SUMMARY OF OPINIONS

12. Based on my analysis of the documents Prudential, Assurance IQ, and ActiveProspect have produced in discovery, my review of publicly available information, my own testing, and my experience, I offer the following opinions:

   a. **Opinion 1**: My testing and analysis show that Prudential and Assurance IQ installed ActiveProspect's source code on its website to intercept in real time data users input into Prudential's webform (e.g., name, email address, phone number, zip code, gender, marital status, date of birth, height, weight, medication status) and sent it to ActiveProspect. I refer to the information that users input into Prudential's webform as "user form input data" or "form input data."

   b. **Opinion 2**: My testing and analysis show that data in possession of Prudential, Assurance IQ, and ActiveProspect can be used to identify natural persons whose form input data was intercepted by ActiveProspect when they filled out a webform to request a life insurance quote on Prudential's website during the Class Period.

IV.   OPINION # 1: PRUDENTIAL AND ASSURANCE IQ INSTALLED ACTIVEPROSPECT'S SOURCE CODE ON PRUDENTIAL'S WEBSITE TO INTERCEPT IN REAL TIME USER FORM INPUT DATA AND SEND IT TO ACTIVEPROSPECT

13. I understand that Prudential and its subsidiary, Assurance IQ, collaborated on the creation and maintenance of Prudential's webform at issue in this case, term.prudential.com.[1]

14. My testing and analysis of Prudential's website[2] showed that it included a section located at https://term.prudential.com/life where a person can fill a form to get an insurance quote.

---

[1] Prudential's Responses to Requests for Admission No. 1 (admitting that "Assurance IQ is a wholly owned subsidiary of Prudential Financial, Inc. and that Assurance IQ, at Prudential's request, was primarily responsible for the creation and maintenance of term.prudential.com."); *id.* No. 6 (admitting that "Prudential Financial, Inc. had ultimate[] authority over term.prudential.com").

[2] It is my understanding that Prudential has now (at the time of writing in June 2024) taken down the life insurance webform (https://term.prudential.com/life).

CONTAINS CONFIDENTIAL INFORMATION

15. Defendants have acknowledged,[3] and my testing confirms, that the TrustedForm script was included in the code for term.prudential.com during the class period.[4]

16. ActiveProspect explains in its End User License Agreement that TrustedForm is "intended to capture what was viewed by the site visitor on the Hosting Page, as well as the site visitor's real-time interactions with the Hosting Page, for example, clicks, mouse movements, and data inputs."[5] ActiveProspect further provides this summary of the script's functionality:

> After the TrustedForm Script is installed on the Hosting Page, when a site visitor visits the Hosting Page, the TrustedForm Script contacts the TrustedForm Server, which then collects information about that site visit . . . and issues a TrustedForm Certificate. The TrustedForm Script also creates a hidden field in the Form that is used to collect and pass the TrustedForm Certificate URL.[6]

17. Below, I show how the TrustedForm software functioned on the Prudential website, which is consistent with ActiveProspect's general description of the software.

18. I describe the events that occur and are triggered by the TrustedForm script (1) when a user navigates to the webform, (2) while the user is interacting with the webform and providing form input data, and (3) when the user submits the form.

WHAT HAPPENS WHEN A USER NAVIGATES TO THE WEBFORM

19. The following figure shows the first webpage of the insurance quote form, which asks a person to tell whether they currently have life insurance.

---

[3] Renz Dep. at 286.

[4] My initial testing of Prudential's life insurance quote webpage was conducted in November 2023, which is outside the class period. However, evidence from the Internet Archive's Wayback Machine (https://web.archive.org/web/20210401000000*/https://term.prudential.com/life) shows that the TrustedForm source code that I analyzed in November 2023 was similarly included by Prudential throughout the Class Period. The technical functionality of TrustedForm's source code, as I describe below, is the same as it was during the Class Period.

[5] AP0000039 (TrustedForm End User License Agreement last updated 4/14/2021).

[6] *Id.*

Figure: The first webpage of the life insurance quote form on Prudential's website.

20. When a website visitor navigates to the first page of the life insurance quote form, the HTML source code for this initial page has commands to include TrustedForm on the webpage as shown in the following figure. Specifically, it includes commands to:

   a. create a "trustedFormFormElement,"

   b. download the initial TrustedForm JavaScript source code,[7] and

   c. check whether the user has JavaScript disabled.

Figure: Excerpt from the HTML source code for Prudential's life insurance quote webpage

---

[7] https://cdn.assurance.com/insurance/public/assets/trustedForm-4a1205758bed9df95ef0ff78d02f73edd84361c32de02c6addd014f63fde670a.js

21. The initial TrustedForm script (hosted by Assurance IQ on https://cdn.assurance.com) further downloads two additional JavaScript source code files from ActiveProspect, at https://cdn.trustedform.com: (1) bootstrap.js[8] and (2) trustedform-1.9.4.js.[9]

22. TrustedForm's JavaScript source code then initiates a series of more than one hundred POST[10] requests that intercept user form input data and send it to TrustedForm's server at https://api.trustedform.com/certs. ActiveProspect itself describes these POST requests as "a series of exchanges that occur in the background while the consumer has the page open."[11] I describe a few categories of POST requests below.

23. The first category of POST request transmitted to TrustedForm's server from Prudential's website contains the information necessary to set up a TrustedForm certificate ("cert"). TrustedForm defines a certificate as a "collection of all the information necessary to document a consumer's interaction with a lead generation form."[12] The payload (or content) of the "cert" POST request includes a JSON object,[13] which is shown in the figure below. It includes:

   a. Configuration parameters of TrustedForm certificate

   b. TrustedForm version

   c. Full URL of the webpage

   d. Browser and screen width and height

   e. User agent string containing device and operating system information. (A user agent string is identifies a web browser's device and operating system).

24. There is only one "cert" POST request to TrustedForm's server, which occurs at the start of a website visitor's interaction with the first page of the webform.

---

[8] https://cdn.trustedform.com/bootstrap.js?provide_referrer=false&field=xxTrustedFormCertUrl&l=17013362437130.2550676600214141&invert_field_sensitivity=false

[9] https://cdn.trustedform.com/trustedform-1.9.4.js

[10] A POST is typically used to upload or send data from a web browser to a web server. https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/POST.

[11] AP00000610.

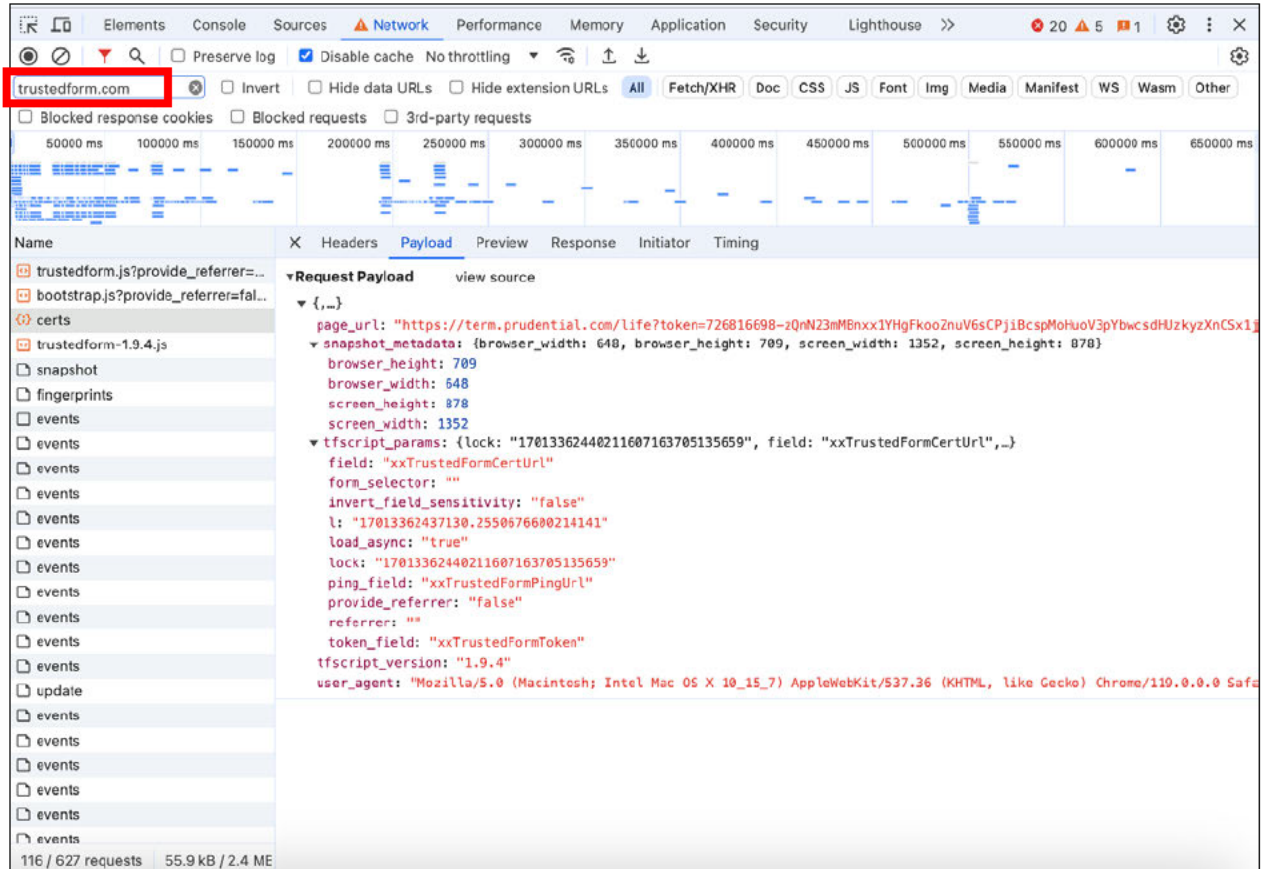[12] https://developers.activeprospect.com/docs/trustedform/getting-started/

[13] JSON is a widely used way to store data in a standard human-readable text format that is also amenable to automated machine parsing. See https://developer.mozilla.org/en-US/docs/Glossary/JSON

Figure: Payload of the "certs" POST request sent to TrustedForm's server

25. The second category of POST request to TrustedForm's server includes a "snapshot" of the website's HTML. The payload of the "snapshot" POST request includes a JSON object shown in the figure below. It includes:

   a. A copy of the website's HTML's Document Object Model (DOM)[14] representation in the web browser

   b. The format in which the "snapshot" is encoded

---

[14] https://developer.mozilla.org/en-US/docs/Web/API/Document_Object_Model ("The Document Object Model (DOM) connects web pages to scripts or programming languages by representing the structure of a document—such as the HTML representing a web page—in memory. Usually it refers to JavaScript, even though modeling HTML, SVG, or XML documents as objects are not part of the core JavaScript language. The DOM represents a document with a logical tree. Each branch of the tree ends in a node, and each node contains objects. DOM methods allow programmatic access to the tree. With them, you can change the document's structure, style, or content.")

CONTAINS CONFIDENTIAL INFORMATION

26. The copy of the website's HTML's DOM representation[15] allows Trustedform to re-create the webpage as it is shown in the user's web browser.

27. ActiveProspect internally describes the snapshot as █████████████████████ ██ ██[16]

28. There is only one "snapshot" POST request to TrustedForm's server, which occurs at the start of a website visitor's interaction with the first page of the webform. The document "Translated Snapshot Payload" contains the decoded payload of the "snapshot" POST request and the Python script I used to this end is "Translate TrustedForm Python Script."
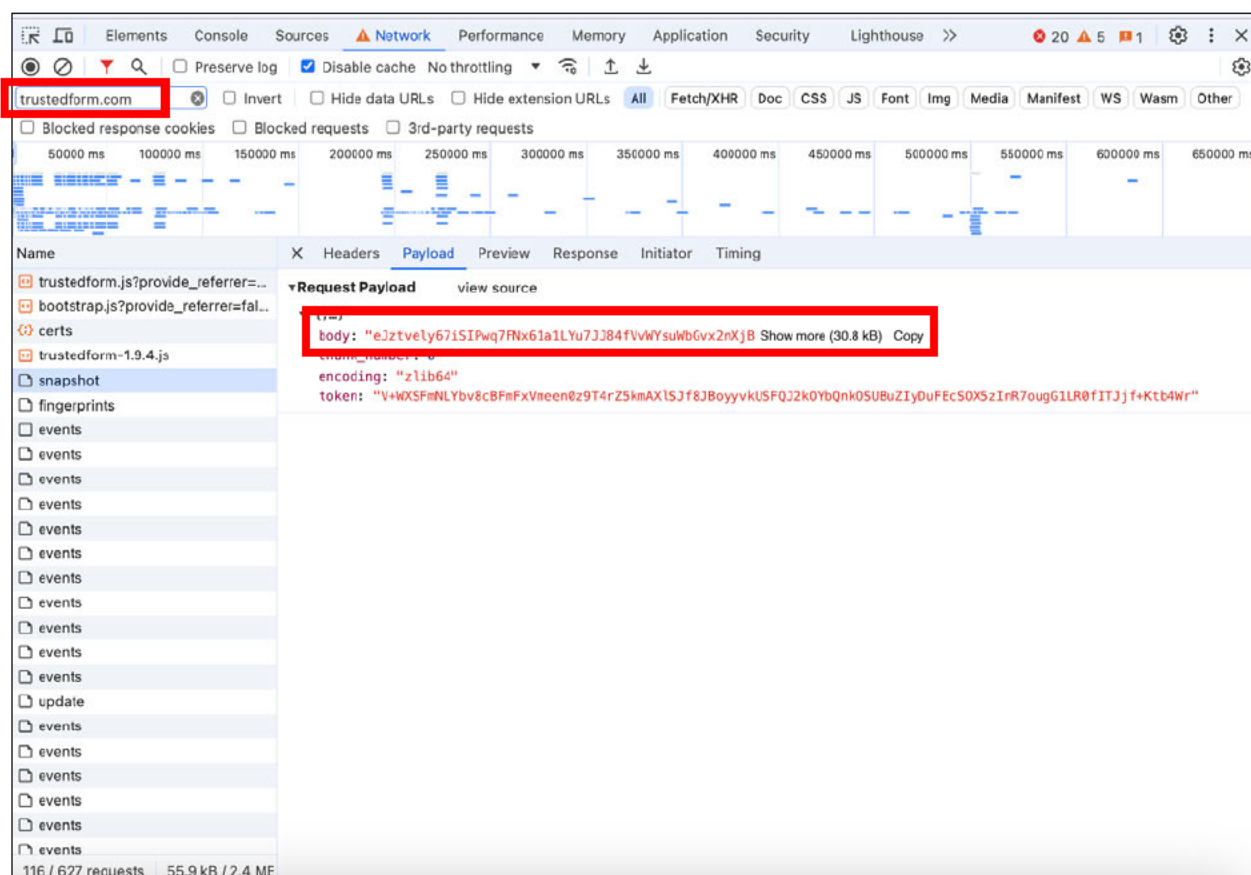
Figure: Payload of the "snapshot" POST request sent to TrustedForm's server

---

[15] The DOM represents an HTML document as a tree of nodes, where each node is an object representing a part of the document (elements, attributes, text, etc.). The DOM tree nodes include all textual content in text nodes, images in .img elements, scripts as script elements, as well as visual styles of elements.
[16] AP0000392

WHAT HAPPENS WHILE A USER INTERACTS WITH THE WEBFORM

29. The third category of POST request to TrustedForm's server includes updates about "events" on the website's HTML. The payload of the "events" POST request includes a JSON object shown in the figure below. It includes:

    a. A copy of the list of updates to the website's HTML's DOM representation in the web browser

    b. The format in which the "event" is encoded

30. Unlike the first two categories of POST requests described above, which occur when the visitor first loads the webpage, the "events" requests are sent throughout the visitor's session on the webform, as each "event" occurs.

31. The vast majority of the more than one hundred POST requests sent to TrustedForm's server as a user completes the Prudential webform are "events" that are sent in real time, with frequency ranging from one second to a few seconds.
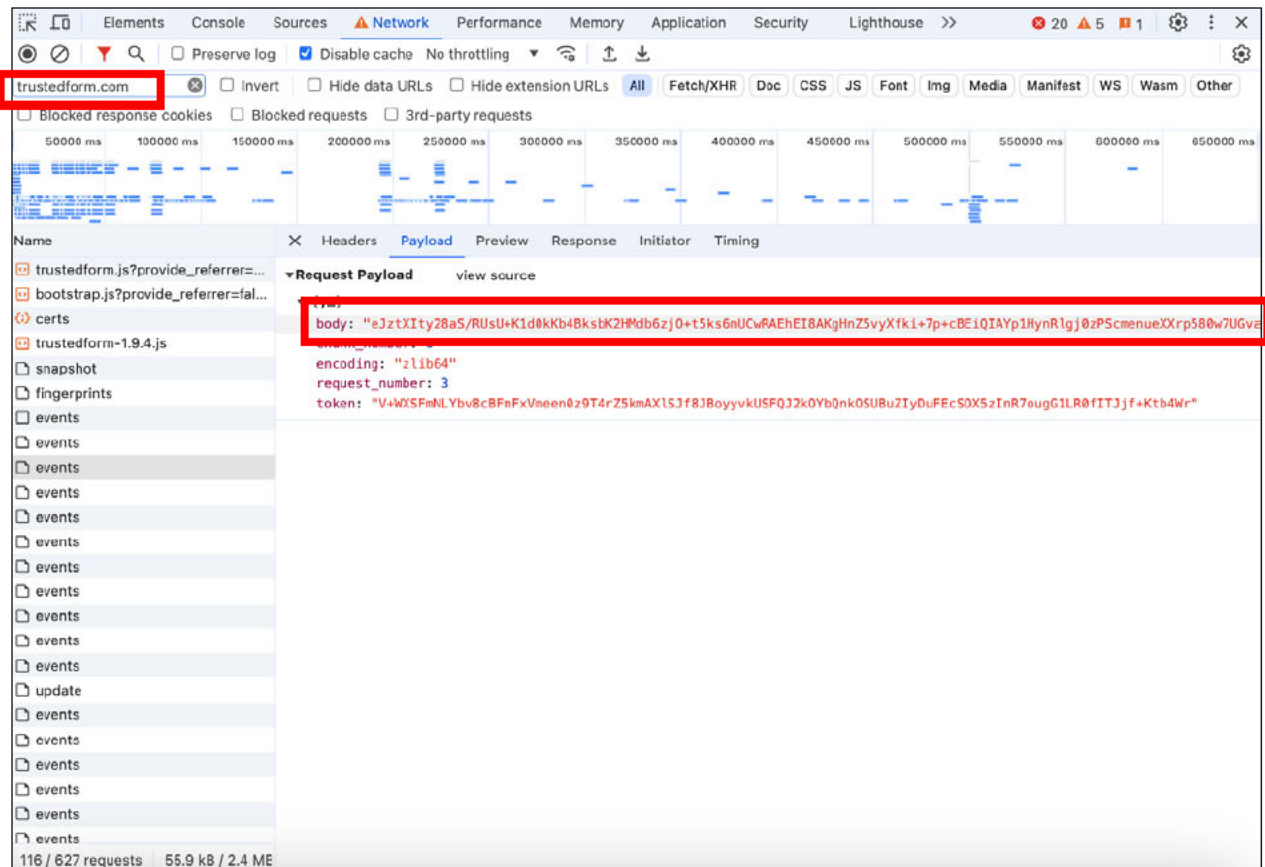
Figure: Payload of an "events" POST request sent to TrustedForm's server

32. As ActiveProspect explains on its website, recorded "events" include every time "the consumer moves or clicks their cursor or presses keys."[17]

33. Each update to the website's HTML's DOM representation allows TrustedForm to re-create the updated version of the webpage as it is currently shown in the user's web browser. In other words, the series of event updates allow TrustedForm to re-create a visual depiction of each action the user took on the webpage.

34. To collect the form data from Prudential's website and generate a replay of the user's visit to the webpage, ActiveProspect uses a technology called "event listeners,"[18] which **listen** to various "events"[19] occurring in a user's web browser in real-time and contemporaneous with the loading of the webpage.

35. Specifically, TrustedForm's source code[20,21] ███████████████████████ ███████████████████████████ ████████████ ███████ ███ ████████ ██████████████████████████ ███████████████████████

36. ██ are instantaneously (i.e., in real-time and without any delay) triggered when these events occur while a user fills out different sections of the life insurance quote request form on Prudential's website.

---

[17] AP0000610.

[18] https://developer.mozilla.org/en-US/docs/Web/API/EventTarget/addEventListener.

[19] https://developer.mozilla.org/en-US/docs/Web/API/Event ("An event can be triggered by the user action e.g. clicking the mouse button or tapping keyboard, or generated by APIs to represent the progress of an asynchronous task."); *id.* ("Many DOM elements can be set up to accept (or 'listen' for) these events, and execute code in response to process (or 'handle') them. Event-handlers are usually connected (or 'attached') to various HTML elements (such as <button>, <div>, <span>, etc.) using EventTarget.addEventListener(), and this generally replaces using the old HTML event handler attributes.").

[20] https://cdn.trustedform.com/trustedform-1.9.4.js

[21] ActiveProspect produced the non-minified version of the JavaScript source code at AP0000239

[22] https://developer.mozilla.org/en-US/docs/Web/API/Element/keydown_event ("The keydown event is fired when a key is pressed.").

[23] https://developer.mozilla.org/en-US/docs/Web/API/Element/click_event ("An element receives a click event when any of the following occurs • a pointing-device button (such as a mouse's primary button) is both pressed and released while the pointer is located inside the element. • a touch gesture is performed on the element • the Space key or Enter key is pressed while the element is focused").

[24] https://developer.mozilla.org/en-US/docs/Web/API/Document/scroll_event

[25] https://developer.mozilla.org/en-US/docs/Web/API/MutationObserver

37. ActiveProspect admits that ███
██
██
██
██[26]

38. ActiveProspect describes on its website that these timestamped events are bundled and sent from the user's browser to ActiveProspect's server "every few seconds" as the user continues to navigate through the webform.[27]

39. On term.prudential.com, the payload of "events" POST requests include all questions on the webform and the user's answers to the questions. These questions[28] include:

    a. "Do you currently have Life Insurance?" ["Yes/No"]

    b. "What is your gender?" ["Female/Male"]

    c. "Have you used Tobacco Products within the last 12 months?" ["Yes/No"]

    d. "Are you currently married?" ["Yes/No"]

    e. "Do you have children?" ["Yes/No"]

    f. "What is your date of birth?" ["Month/DD/YYY"]

    g. "Why are you looking for life insurance?" ["Financially support loved ones/Cover debts/etc"]

    h. "What is your height?" ["ft'in'"]

    i. "What is your weight?" ["Pounds"]

    j. "Are you currently taking any prescription medications?" ["Yes/No"]

    k. "In the past 5 years have you been treated or prescribed medication for any of the following conditions?" ["Anxiety / Depression / Bipolar", "Heart or circulatory disorder", "Cancer", "Respiratory disorder", "Chronic pain", "Other medical condition"]

    l. "Have you been hospitalized or missed more than 1 week of work due to anxiety, depression, or bipolar disease?" ["Yes/No"]

    m. "Are you currently employed?" ["Currently employed/Student"]

---

[26] AP0000392

[27] AP0000768.

[28] *See, e.g.*, PRU0000097.

n. "Did you have an amount of coverage in mind?" ["Over 500K"]

o. "What is your zipcode?" ["zip"]

p. "What is your name?" ["First Name", "Last Name"]

q. "What is your email?" ["Email"]

r. "Last step! Your quote is ready. Please enter your mobile number." ["Phone"]

40. The following excerpt of the payload of an "events" POST request shows that it contains the question "Are you currently married?" and the answer selected by user. Similarly, it also shows the email address I provided on the webform in response to "What is your email?". The document "Translated Events Payload" contains the decoded payloads of all "events" POST requests and the python script I used to this end is "Translate TrustedForm Python Script."

```
▼ 7 {4}
    t   : 3
    p   : 782
    id  : 783
    v     Are you currently married?
```

```
▼ 10 {5}
    t   : 1
    p   : 785
    id  : 786
    n   : label
    ▼       [4]
        0 : class
        1 : radio-container
        2 : for
        3 : married_true
```
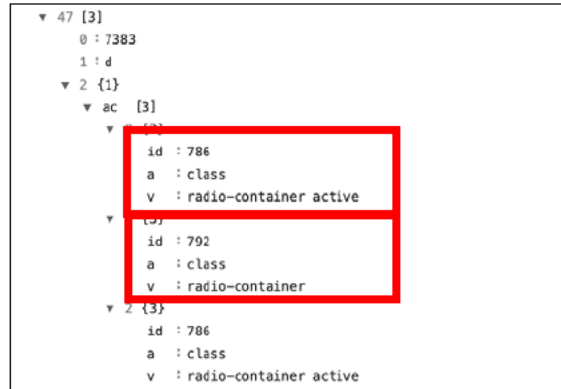
```
▼ 16 {5}
    t   : 1
    p   : 791
    id  : 792
    n   : label
    ▼       [4]
        0 : class
        1 : radio-container
        2 : for
        3 : married_false
```

```
▼ 47 [3]
    0 : 7383
    1 : d
  ▼ 2 {1}
    ▼ ac  [3]
      ▼
          id  : 786
          a   : class
          v   : radio-container active
      ▼
          id  : 792
          a   : class
          v   : radio-container
      ▼ 2 {3}
          id  : 786
          a   : class
          v   : radio-container active
```

Figure: Excerpt of the decoded HTML DOM in the payload of an "events" POST request. The element ID 786 represents "married_true" and 792 represents "married_false". The user's choice is represented by the fact that the "active" radio-container is 786, not 792.


```
▼ 1 [4]
    0 : 214362
    1 : k
    2 : 1847
    3   zubairch@gmail.com
```

Figure: Excerpt of the decoded HTML DOM in the payload of an "events" POST request. It contains the email address I provided in plaintext.

41. The fourth category of POST request to TrustedForm's server includes a "fingerprints" POST request, which transmits the email address entered by a user in the form. The payload of the "fingerprints" POST request includes a JSON object shown in the figure below. It includes:

    s.   Different hashes of email address using SHA-1[29]

42. The information sent to TrustedForm in hashed format in the "fingerprints" POST request is also sent in plaintext in the "events" POST requests. Thus, the hashed PII[30] is duplicative of the unhashed PII.

---

[29] Hashing refers to a method of creating a unique digest from an input. SHA-1 is a particular method used for hashing. https://developer.mozilla.org/en-US/docs/Glossary/Cryptographic_hash_function

[30] Even if an unhashed version of the PII were not also included, it is straightforward to reverse the hash of inputs such as names, email addresses, or phone numbers using a well-known, decade-old technique. Essentially, one can quickly and cheaply compute the hash of all known names, email addresses, or phone numbers and store them in a table. A typical personal computer costing less than $1000 can compute more than 16 billion SHA-1 hashes in one second. It is simple for anyone to brute-force SHA-1 hashes of hundreds of billions of names, email addresses, or phone numbers in a few minutes. Once this table is ready, one can quickly lookup the SHA-1 hash in the table and find the corresponding name, email

43. The fingerprint "049a36a273b268b7bfb3769b854dad3cbdc9e618" in the figure below is the SHA-1 hash of the email address "zubairch@gmail.com" in the figure above.
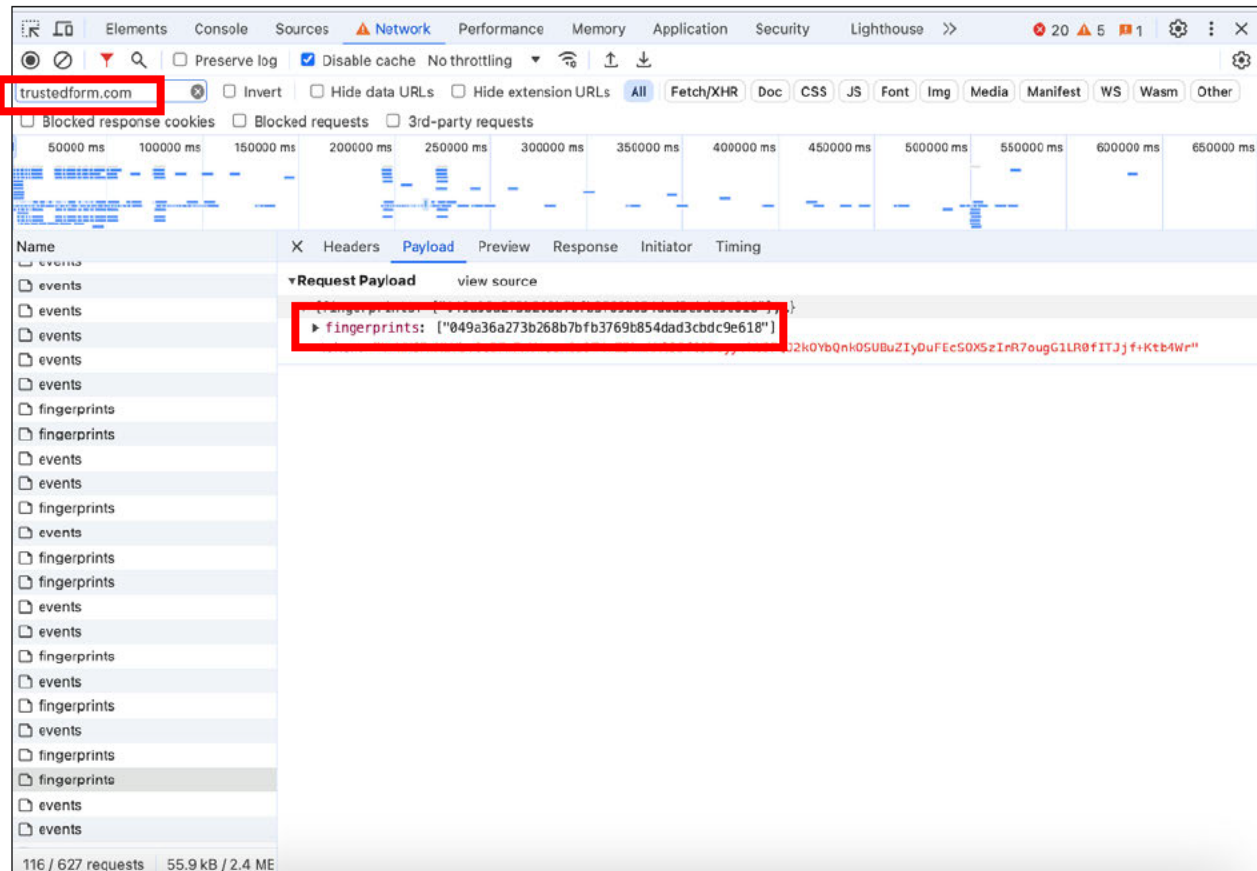
Figure: Payload of a "fingerprints" POST request sent to TrustedForm's server. The fingerprint "049a36a273b268b7bfb3769b854dad3cbdc9e618" is the SHA1 hash of the email address "zubairch@gmail.com"

44. The fifth category of POST requests to TrustedForm's server includes "updates" about user interaction on the webpage. The payload of the "updates" POST request includes a JSON object shown in the figure below. It includes:

   t.   Form input method (e.g., "typing")

   u.   Typing speed in keys-per-minute and words-per-minute

---

address, or phone number. In fact, there are several companies that provide an email hash lookup service for a few cents.

CONTAINS CONFIDENTIAL INFORMATION
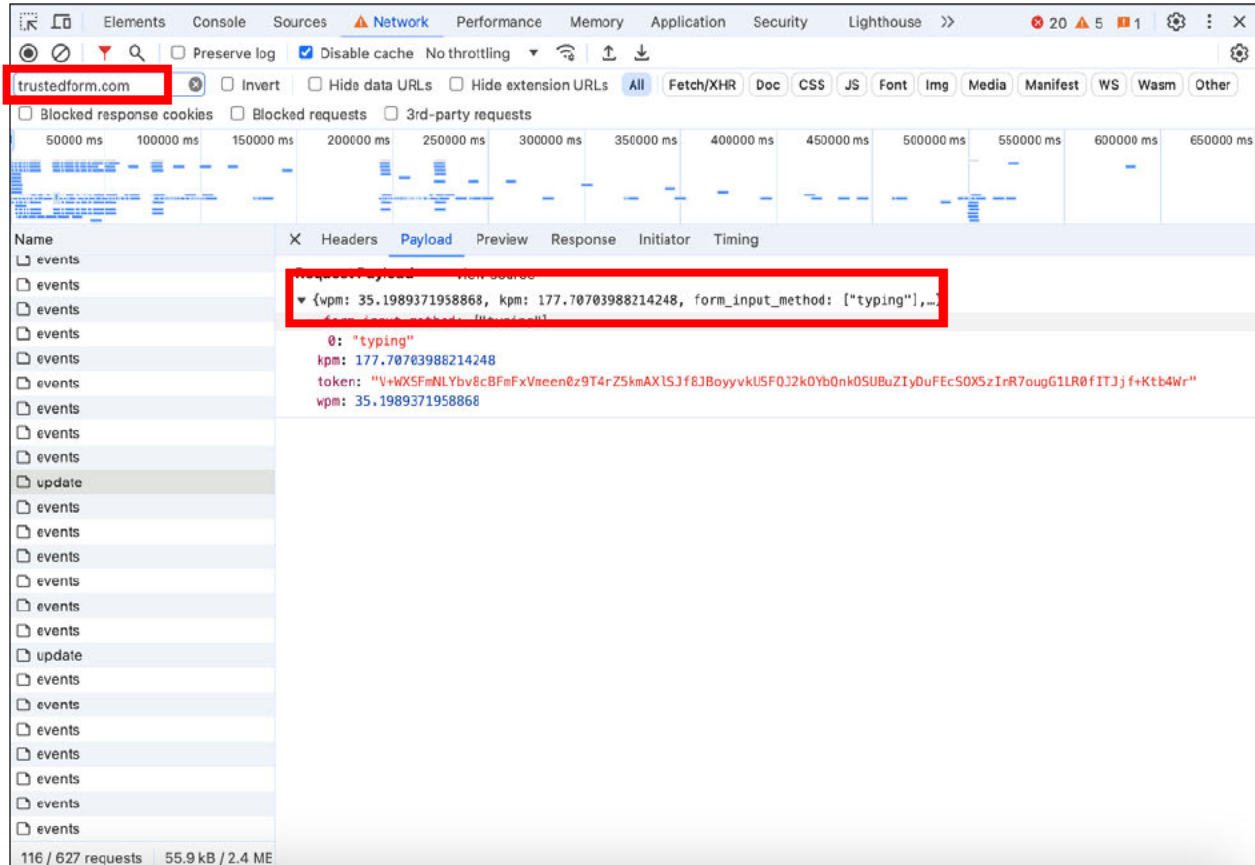
Figure: Payload of an "update" POST request sent to TrustedForm's server

WHAT HAPPENS WHEN A USER SUBMITS THE WEBFORM

45. ActiveProspect describes what happens when a user completes and submits a webform using TrustedForm as follows:

> When the consumer either abandons the page or submits a form (which also causes page abandonment) the connection between the user's browser and the TrustedForm service closes. At this point TrustedForm saves everything that the browser has sent up to it. This is the TrustedForm Certificate. It retrieves any additional files specified in the DOM from their respective servers and adds them to the Certificate, which is now complete.[31]

46. During the initial connection, the TrustedForm Script created "a hidden field in the Form that is used to collect and pass the TrustedForm Certificate URL." When a site visitor

---

[31] AP0000610.

CONTAINS CONFIDENTIAL INFORMATION

"completes the Form and submits his/her information (thereby generating a Lead), then the TrustedForm Certificate URL, within that hidden field, should be collected and sent with the rest of the Lead data."[32]

47. On term.prudential.com, Assurance IQ maintained a database that collected the information submitted by visitors to the webform.[33] ███████████████████████
██.[34]

BUILDING THE SESSION REPLAY VIDEO

48. All of the data shown in the preceding paragraphs is intercepted by ActiveProspect in real time and allows it to create a video recording of a user responding to each question posed by the webform on Prudential's website. For example, PRU0000097 is a video recording generated by ActiveProspect and produced by Prudential for a named plaintiff in this matter corresponding to a certificate stored by ActiveProspect.

49. The kind of tracking technology used by ActiveProspect is called session replay, which allows website developers to observe "how their page was rendered for the user and how the user interacted with their site." [35][36]

50. In fact, ActiveProspect publicly describes TrustedForm as a "session replay" technology that "documents every keystroke and every step of the consumer interaction on the page, as well as information about when and where the form was completed."[37]

51. ActiveProspect's list[38] of the data collected by TrustedForm includes

    a. "Time form was loaded by consumer",

    b. "The consumers public IP address",

    c. "Latitude and longitude based on IP location"

---

[32] *Id.*

[33] Renz Dep. at 71-72.

[34] *See, e.g.*, PRU0002712; PRU0002714 (database entries for the named plaintiffs).

[35] Acar, G., Englehardt, S. and Narayanan, A., 2020. No boundaries: data exfiltration by third parties embedded on web pages. Proceedings on Privacy Enhancing Technologies.

[36] Senol, A., Acar, G., Humbert, M. and Borgesius, F.Z., 2022. Leaky forms: A study of email and password exfiltration before form submission. In 31st USENIX Security Symposium (USENIX Security 22) (pp. 1813-1830).

[37] https://activeprospect.com/resources/discovering-trustedform-api/

[38] https://activeprospect.com/resources/discovering-trustedform-api/

d.   "City based on IP location"

e.   "Country based on IP location"

f.   "Consumer User agent data, raw string"

g.   "Web address where the form was located"

h.   "Base domain address of the URL"

i.   "How form was filled (ex. Typing, autofill, or copy/paste)"

j.   "Keystrokes per minute (consumer's typing speed on form)"

k.   "Words per minute (consumer's typing speed on form)", and

l.   "View of the consumer completing the form".

52. As explained earlier, TrustedForm's source code was included on Prudential's life insurance quote request form during the class period. This means that TrustedForm's source code was loaded and ready for data collection (e.g., through the aforementioned "listeners") as soon as a user starts filling out the life insurance form.

53. The following figure plots the timeseries of the transmissions from the web browser to servers when a user fills out all sections of the form on Prudential's website. The red lines indicate the transmissions to TrustedForm's server. The blue lines indicate the transmissions from the web browser to all other servers. As this graphic demonstrates, the POST requests to TrustedForm's server occur contemporaneously as a user fills out the life insurance form on Prudential's website.
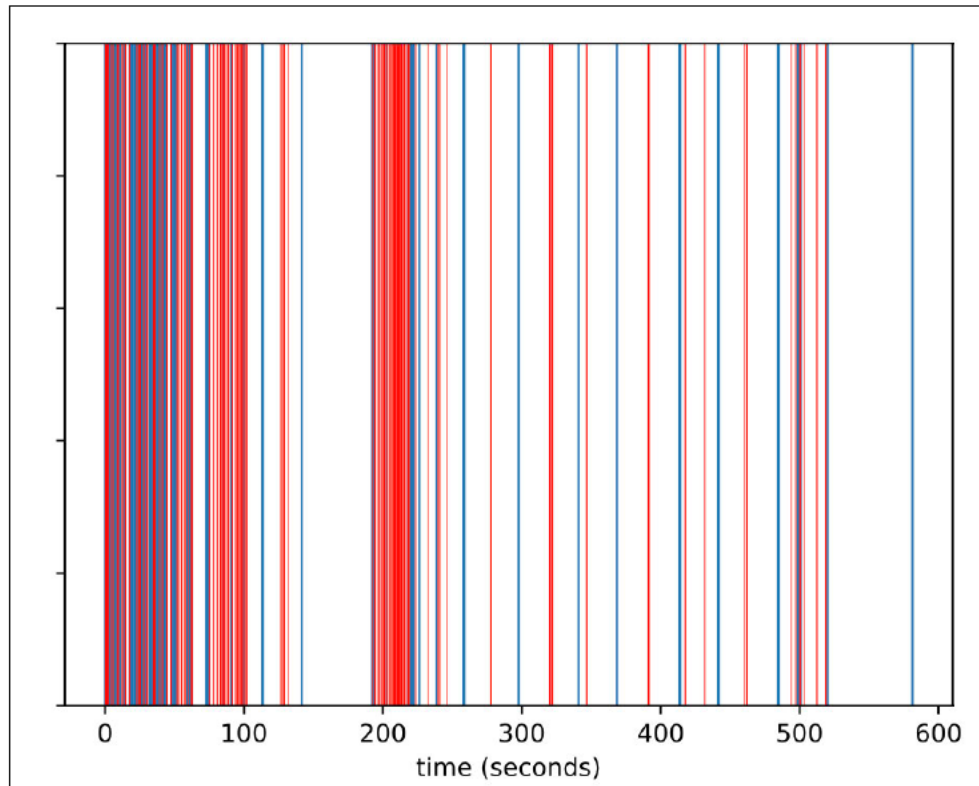
Figure: Timeseries of requests as a user fills out life insurance form on Prudential's website. The red lines represent the transmissions to TrustedForm's server.

54. Based on the foregoing, I conclude that Prudential and Assurance IQ installed ActiveProspect's source code on Prudential's website to intercept in real time user form input data (e.g., name, email address, phone number, zip code, gender, marital status, date of birth, height, weight, medication status) and sent it to ActiveProspect.

V.   **OPINION # 2: DATA IN POSSESSION OF PRUDENTIAL, ASSURANCE IQ, AND ACTIVEPROSPECT CAN BE USED TO IDENTIFY NATURAL PERSONS WHOSE DATA WAS INTERCEPTED BY ACTIVEPROSPECT WHEN THEY FILLED OUT A WEBFORM TO REQUEST A LIFE INSURANCE QUOTE ON PRUDENTIAL'S WEBSITE DURING THE CLASS PERIOD**

55. I have been asked by Counsel to investigate whether data in possession of Prudential, Assurance IQ, and ActiveProspect can be used to identify natural persons whose data was

intercepted by ActiveProspect when they filled out a webform to request a life insurance quote on Prudential's website during the Class Period.

56. I first analyze whether a user's browser impacts the functioning of Trusted Form and whether determination of the class will be complicated by persons who block cookies, persons who disable javascript, or the presence of bots.

57. ActiveProspect's CEO testified that the operation of TrustedForm does not vary based on whether the visitor to a website is a mobile or a desktop user, what their cookie settings are, and what web browser they use. [39] This is consistent with my investigation.

TrustedFrom's JavaScript Source Code is Browser Agnostic

58. To this end, I first analyze whether the interception by TrustedForm script is browser agnostic – i.e., it works the same in all major web browsers. The four major web browsers in the United States include Google Chrome, Microsoft Edge, Apple Safari, and Mozilla Firefox, which together account for more than 95% of the market share in the United States. [40,]

59. All four of these major web browsers natively support JavaScript, including the capabilities to setup "listeners"[41] and "observers".[42]

Cookie Blocking Software Does Not Impact the Functionality of TrustedForm

60. "A cookie is a small piece of information left on a visitor's computer by a website, via a web browser."[43]

61. My review of TrustedForm's JavaScript source code indicates that it does not make use of any browser cookies. This is confirmed by my observation that none of the POST

---

[39] Rafferty Dep. 140-42.

[40]https://gs.statcounter.com/browser-market-share/all/chart.php?device=Desktop%20%26%20Mobile%20%26%20Tablet%20%26%20Console&device_hidden=desktop%2Bmobile%2Btablet%2Bconsole&multi-device=true&statType_hidden=browser&region_hidden=US&granularity=monthly&statType=Browser&region=United%20States%20of%20America&fromInt=202304&toInt=202404&fromMonthYear=2023-04&toMonthYear=2024-04&csv=1

[41] https://developer.mozilla.org/en-US/docs/Web/API/EventTarget/addEventListener#browser_compatibility

[42] https://developer.mozilla.org/en-US/docs/Web/API/MutationObserver#browser_compatibility

[43] https://developer.mozilla.org/en-US/docs/Glossary/Cookie

requests sent to TrustedForm's server include any cookies in the Cookie header.[44] Thus, I conclude that the interception by TrustedForm's JavaScript source code is not impacted by cookie blocking software.[45]

People Who Disable JavaScript Are Not Included in the Class

62. The only meaningful way to stop interception by TrustedForm's JavaScript source code is to block TrustedForm's JavaScript by disabling all JavaScript in the user's web browser settings.[46]

63. Peer-reviewed research has shown that blocking JavaScript breaks website functionality.[47] The researchers found that blocking JavaScript results in major functionality breakage on approximately two-thirds of the websites. This is not surprising because almost all websites heavily rely on JavaScript to implement different types of functionalities.[48]

64. Thus, I conclude that a negligible fraction of users would disable JavaScript because it would prevent them from using most of the websites that exist today.

65. In any event, I understand the class to be limited to persons for whom a TrustedForm Certificate URL was generated. No TrustedForm certificate would be generated for anyone who disabled JavaScript because there would not by any POST requests to TrustedForm's server – including the "cert" POST request.

66. Thus, people who disabled JavaScript would be excluded from the class if the presence of a Trusted Form certificate is used to determine class membership.

Bots Are Unlikely to Complete the Webform and Are Excluded from the Class

67. Discovery shows that Assurance used multiple services to prevent bots[49] from filling out its forms.[50] Specifically, Kevin Bao, an Assurance IQ employee, testified that Assurance

---

[44] https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cookie
[45] https://webkit.org/tracking-prevention/#intelligent-tracking-prevention-itp
[46] https://www.computerhope.com/issues/ch000891.htm
[47] Amjad, A.H., Shafiq, Z. and Gulzar, M.A., 2023, January. Blocking JavaScript without Breaking the Web. In Privacy Enhancing Technologies Symposium (PETS).
[48] https://almanac.httparchive.org/en/2022/javascript
[49] A bot is a computer program that can automatically interact with a webpage and do certain tasks. https://www.cloudflare.com/learning/bots/what-is-a-bot/
[50] Bao Dep. at 150-51.

██

███

68. ███ ███ ███

██

███

███████████████ ██

██

██████████████████ ███████████████████████████████████

███

███

███

██████████████ █

69. ███████████████████████████████████████ ███ ████████

███

███

███

██

███████████████ ███

███████████████████████

70. It is unlikely that many, if any, bots successfully completed the webform at
term.prudential.com in the class period, because of the state-of-the-art[60,61] defenses

---

51 ███████████████████████
██ ██
██ ██
██ ████████████████████████████████
██ ███
██ ███
██ ██
██ ██
██ ██
█ ██

described above were in place and because of the complexity and multi-page nature of the webform on term.prudential.com. Even if a bot got through a portion of the webform, it is unlikely that a bot would be able to navigate all the way to the end and submit the form in a way that it will trigger the TrustedForm script.[62]

Records from Prudential, Assurance IQ, and ActiveProspect Can Be Used to Identify Class Members

71. Discovery shows that Prudential and Assurance IQ have a database of people who submitted the relevant webform and whose submission has TrustedForm certificate associated with it.

72. Assurance IQ maintained a database that collected the information submitted by visitors to the webform.[63] ████████████████████████████████
██
██
██
██████████

73. ActiveProspect also stores the TrustedForm certificates in its own database.[65]

74. These databases of form submissions and TrustedForm certificates can be used to reliably identify persons whose information was intercepted by ActiveProspect in California.

75. Both Assurance IQ's database and ActiveProspect's TrustedForm Certificates document the user's IP address, which identify the user's geolocations and thus can be used to identify webform submissions that were sent from California.

76. Prudential produced the session replay video for the plaintiff Valerie Torres that corresponded to the certificate ID ████████████████████████████[66] The

██
██
██

---

[62] Rafferty Dep. at 130.
[63] Renz Dep. at 71-72; Bao Dep. at 65.
[64] *See, e.g.*, PRU0002712; PRU0002714 (database entries for the named plaintiffs); Bao Dep. at 65.
[65] Rafferty Dep. at 53; 77.
[66] PRU0000097

video included PII, such as the name, email address, and phone number, which can be used to identify a class member. The same process can be repeated for all session replay videos in Prudential's possession to identify class members.

77. In addition to reviewing the certificates themselves, any natural person who submitted Prudential's webform and whose visit was recorded by TrustedForm will have a TrustedForm Certificate URL associated with their entry in Assurance IQ's database.

78. Based on the foregoing, I conclude that the data in possession of Prudential, Assurance IQ, and ActiveProspect can be used to identify natural persons whose data was intercepted by ActiveProspect when they filled out a webform to request a life insurance quote on Prudential's website during the Class Period.

DATED: June 28, 2024   _____

                                        Zubair Shafiq

APPENDIX A

Zubair Shafiq

3043 Kemper Hall
Davis, CA, 95616 USA
✉ *zubair@ucdavis.edu*
🌐 *www.cs.ucdavis.edu/~zubair*

▬▬▬ Research Interests

Web Privacy, Internet Measurement, Internet Security, Computer Networks

▬▬▬ Professional Experience

2020–	**Associate Professor**
	Department of Computer Science, University of California-Davis
2014–2020	**Assistant Professor**
	Department of Computer Science, University of Iowa
2009–2014	**Research Assistant**
	Department of Computer Science and Engineering, Michigan State University
2013	**Research Intern**
	IBM T. J. Watson Research Center
2012	**Research Intern**
	Telefonica Research
2011	**Research Intern**
	AT&T Labs – Research
2007-2009	**Research Engineer**
	Next Generation Intelligent Networks Research Center, Pakistan

▬▬▬ Education

2009–2014	**Ph.D. Computer Science**
	Department of Computer Science and Engineering, Michigan State University
2004–2008	**B.E. Electrical Engineering**
	National University of Sciences & Technology (NUST), Pakistan

▬▬▬ Honors and Awards

2024	**Caspar Bowden Award**, Runner-up for Outstanding Research in Privacy Enhancing Technologies
2023	**Best Paper Award**, ACM Internet Measurement Conference
2023	**Chancellor's Fellow**, University of California Davis
2020	**Research Highlights**, Communications of the ACM
2020	**Dean's Scholar Award**, University of Iowa
2018	**NSF Faculty Early Career Development (CAREER) Award**
2018	**Andreas Pfitzmann Award**, Best Student Paper at Privacy Enhancing Technologies Symposium
2017	**Best Paper Award**, ACM Internet Measurement Conference
2015	**NSF CISE Research Initiation Initiative (CRII) Award**
2013	**Fitch-Beach Outstanding Graduate Research Award**, Michigan State University
2012	**Best Paper Award**, IEEE International Conference on Network Protocols

2007, 2008 **Dean's Plaque of Excellence**, National University of Sciences & Technology, Pakistan

Publications

CCS   **Blocking Tracking JavaScript at the Function Granularity**
Abdul Haddi Amjad, Shaoor Munir, Zubair Shafiq, Muhammad Ali Gulzar
ACM Conference on Computer and Communications Security, 2024 (in press)

USENIX   **PURL: Safe and Effective Sanitization of Link Decoration**
Security   Shaoor Munir, Patrick Lee, Umar Iqbal, Zubair Shafiq, Sandra Siby
USENIX Security Symposium, 2024 (in press)

JETLaw   **Google's Chrome Antitrust Paradox**
Shaoor Munir, Konrad Kollnig, Anastasia Shuba, Zubair Shafiq
Vanderbilt Journal of Entertainment and Technology Law, 2024 (in press)

IMWUT/   **Aragorn: A Privacy-Enhancing System for Mobile Cameras**
UbiComp   Hari Venugopalan, Zainul Abi Din, Trevor Carpenter, Jason Lowe-Power, Sam King, Zubair Shafiq
ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2024 (in press)

CHI   **Understanding Underground Incentivized Review Services**
Rajvardhan Oak, Zubair Shafiq
ACM Conference on Human Factors in Computing Systems, 2024

S&P   **The Inventory is Dark and Full of Misinformation: Understanding the Abuse of Ad Inventory Pooling in the Ad-Tech Supply Chain**
Yash Vekaria, Rishab Nithyanand, Zubair Shafiq
IEEE Symposium on Security & Privacy, 2024

JOLT   **A Scientific Approach to Tech Accountability**
Woodrow Hartzog, Scott Jordan, David Choffnes, Athina Markopoulou, Zubair Shafiq
Beyond the FTC: The Future of Privacy Enforcement, Harvard Journal of Law & Technology, 2023

PNAS   **Auditing YouTube's Recommendation System for Ideologically Congenial, Extreme, and Problematic Recommendations**
Muhammad Haroon, Magdalena Wojcieszak, Anshuman Chhabra, Xin Liu, Prasant Mohapatra, Zubair Shafiq
Proceedings of the National Academy of Sciences (PNAS), 2023

IMC   **Tracking, Profiling, and Ad Targeting in the Alexa Echo Smart Speaker Ecosystem**
Umar Iqbal, Pouneh Nikkhah Bahrami, Rahmadi Trimananda, Hao Cui, Alexander Gamero-Garrido, Daniel Dubois, David Choffnes, Athina Markopoulou, Franziska Roesner, Zubair Shafiq
ACM Internet Measurement Conference, 2023
Best Paper Award

PETS   **A Utility-Preserving Obfuscation Approach for YouTube Recommendations**
Jiang Zhang, Hadi Askari, Konstantinos Psounis, Zubair Shafiq
Privacy Enhancing Technologies Symposium, 2023

PETS   **Blocking JavaScript without Breaking the Web**
Abdul Haddi Amjad, Zubair Shafiq, Muhammad Ali Gulzar
Privacy Enhancing Technologies Symposium, 2023

CCS   **CookieGraph: Measuring and Countering First-Party Tracking Cookies**
Shaoor Munir, Sandra Siby, Umar Iqbal, Steven Englehardt, Zubair Shafiq, Carmela Troncoso
ACM Conference on Computer and Communications Security, 2023

S&P **Accuracy-Privacy Trade-off in Deep Ensemble: A Membership Inference Perspective**
Shahbaz Rezaei, Zubair Shafiq, Xin Liu
IEEE Symposium on Security & Privacy, 2023

USENIX **AutoFR: Automated Filter Rule Generation for Adblocking**
Security Hieu Le, Salma Elmalaki, Athina Markopoulou, Zubair Shafiq
USENIX Security Symposium, 2023

NDSS **Harpo: Learning to Subvert Online Behavioral Advertising**
Jiang Zhang, Konstantinos Psounis, Muhammad Haroon, Zubair Shafiq
Network and Distributed System Security Symposium, 2022

USENIX **WebGraph: Capturing Advertising and Tracking Information Flows for Robust Blocking**
Security Sandra Siby, Umar Iqbal, Steven Englehardt, Zubair Shafiq, Carmela Troncoso
USENIX Security Symposium, 2022

USENIX **Khaleesi: Breaker of Advertising and Tracking Request Chains**
Security Umar Iqbal, Charlie Wolfe, Charles Nguyen, Steven Englehardt, Zubair Shafiq
USENIX Security Symposium, 2022

PETS **FP-Radar: Longitudinal Measurement and Early Detection of Browser Fingerprinting**
Pouneh Nikkhah Bahrami, Umar Iqbal, Zubair Shafiq
Privacy Enhancing Technologies Symposium, 2022

ACL **Adversarial Authorship Attribution for Deobfuscation**
Wanyue Zhai, Jonathan Rusert, Zubair Shafiq, Padmini Srinivasan
Association for Computational Linguistics, 2022

ACL **On the Robustness of Offensive Language Classifiers**
Jonathan Rusert, Zubair Shafiq, Padmini Srinivasan
Association for Computational Linguistics, 2022

EuroS&P **DNN Model Architecture Fingerprinting Attack on CPU-GPU Edge Devices**
Kartik Patwari, Syed Mahbub Hafiz, Han Wang, Houman Homayoun, Zubair Shafiq, Chen-Nee Chuah
IEEE European Symposium on Security and Privacy, 2022

DATE **Stealthy Inference Attack on DNN via Cache-based Side-channel Attacks**
Han Wang, Syed Mahbub Hafiz, Kartik Patwari, Chen-Nee Chuah, Zubair Shafiq, Houman Homayoun
IEEE/ACM Design Automation and Test in Europe, 2022

IMC **TrackerSift: Untangling Mixed Tracking and Functional Web Resources**
Abdul Haddi Amjad, Danial Saleem, Fareed Zaffar, Muhammad Ali Gulzar, Zubair Shafiq
ACM Internet Measurement Conference, 2021

S&P **Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors**
Umar Iqbal, Steven Englehardt, Zubair Shafiq
IEEE Symposium on Security & Privacy, 2021

NDSS **CV-Inspector: Towards Automating Detection of Adblock Circumvention**
Hieu Le, Athina Markopoulou, Zubair Shafiq
Network and Distributed System Security Symposium, 2021

EACL **Through the Looking Glass: Learning to Attribute Synthetic Text Generated by Language Models**
Shaoor Munirl, Brishna Batool, Zubair Shafiq, Padmini Srinivasan, Fareed Zaffar
European Chapter of the Association for Computational Linguistics, 2021

IMC **Understanding Incentivized Mobile App Installs on Google Play Store**
Shehroze Farooqi, Alvaro Feal, Tobias Lauinger, Damon McCoy, Zubair Shafiq, Narseo Vallina-Rodriguez
ACM Internet Measurement Conference, 2020

ACL **A Girl Has A Name: Detecting Authorship Obfuscation**
Asad Mahmood, Zubair Shafiq, Padmini Srinivasan
Annual Conference of the Association for Computational Linguistics, 2020

S&P **AdGraph: A Graph-Based Approach to Ad and Tracker Blocking**
Umar Iqbal, Peter Snyder, Shitong Zhu, Benjamin Livshits, Zhiyun Qian, Zubair Shafiq
IEEE Symposium on Security & Privacy, San Francisco, 2020

PETS **CanaryTrap: Detecting Data Misuse by Third-Party Apps on Online Social Networks**
Shehroze Farooqi, Maaz Musa, Zubair Shafiq, Fareed Zaffar
Privacy Enhancing Technologies Symposium, Montreal, 2020

PETS **Inferring Tracker-Advertiser Relationships in the Online Advertising Ecosystem**
John Cook, Rishab Nithyanand, Zubair Shafiq
Privacy Enhancing Technologies Symposium, Montreal, 2020

PETS **The TV is Smart and Full of Trackers: Measuring Smart TV Advertising and Tracking**
Janus Varmarken, Hieu Le, Anastasia Shuba, Zubair Shafiq, Athina Markopoulou
Privacy Enhancing Technologies Symposium, Montreal, 2020

IoTDI **Characterizing Smart Home IoT Traffic in the Wild**
M. Hammad Mazhar, Zubair Shafiq
ACM/IEEE Conference on Internet of Things Design and Implementation, Sydney, 2020

PAM **FlowTrace: A Framework for Active Bandwidth Measurements using In-band Packet Trains**
Adnan Ahmed, Ricky Mok, Zubair Shafiq
Passive and Active Measurement Conference, Eugene, 2020

PETS **A Girl Has No Name: Automated Authorship Obfuscation using X-Mutant**
Asad Mahmood, Faizan Ahmad, Zubair Shafiq, Padmini Srinivasan, Fareed Zaffar
Privacy Enhancing Technologies Symposium, Stockholm, 2019

PETS **No Place to Hide: Inadvertent Location Privacy Leaks on Twitter**
Jonathan Rusert, Osama Khalid, Dat Hong, Zubair Shafiq, Padmini Srinivasan
Privacy Enhancing Technologies Symposium, Stockholm, 2019

WWW **Measurement and Early Detection of Third-Party Application Abuse on Twitter**
Shehroze Farooqi, Zubair Shafiq
The Web Conference (WWW), San Francisco, 2019

WWW **ShadowBlock: A Lightweight and Stealthy Adblocking Browser**
Shitong Zhu, Umar Iqbal, Zhongjie Wang, Zhiyun Qian, Zubair Shafiq, Weiteng Chen
The Web Conference (WWW), San Francisco, 2019

WWW **Measuring Political Personalization of Google News Search**
Huyen Le, Raven Maragh, Brian Ekdale, Timothy Havens, Andrew High, Zubair Shafiq
The Web Conference (WWW), San Francisco, 2019

ASONAM **A Postmortem of Suspended Twitter Accounts in the 2016 U.S. Presidential Election**
Huyen Le, Bob Boynton, Zubair Shafiq, Padmini Srinivasan
IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), Vancouver, 2019

TDSC **Large Scale Characterization of Software Vulnerability Life Cycles**
Muhammad Shahzad, Zubair Shafiq, Alex X. Liu
IEEE Transactions on Dependable and Secure Computing, 2019

PETS **NoMoAds: Effective and Efficient Cross-App Mobile Ad-Blocking**
Anastasia Shuba, Athina Markopoulou, Zubair Shafiq
Privacy Enhancing Technologies Symposium, Barcelona, 2018
Andreas Pfitzmann Best Student Paper Award

NDSS **Measuring and Disrupting Anti-Adblockers Using Differential Execution Analysis**
Shitong Zhu, Xunchao Hu, Zhiyun Qian, Zubair Shafiq, Heng Yin
Network and Distributed System Security Symposium, San Diego, 2018

INFOCOM **Real-time Video Quality of Experience Monitoring for HTTPS and QUIC**
M. Hammad Mazhar, Zubair Shafiq
IEEE International Conference on Computer Communications, Honolulu, 2018

TON **Optimizing Internet Transit Routing for Content Delivery Networks**
Faraz Ahmed, Zubair Shafiq, Amir Khakpour, Alex Liu
IEEE/ACM Transactions on Networking, 2018

TBD **Optimizing Taxi Driver Profit Efficiency: A Spatial Network-based Markov Decision Process Approach**
Xun Zhou, Huigui Rong, Chang Yang, Qun Zhang, Amin Vahedian Khezerlou, Hui Zheng, Zubair Shafiq, Alex Liu
IEEE Transactions on Big Data, 2018

TOPS **Measuring, Characterizing, and Detecting Facebook Like Farms**
Muhammad Ikram, Lucky Onwuzurike, Shehroze Farooqi, Emiliano De Cristofaro, Arik Friedman, Guillaume Jourjon, Dali Kaafar, Zubair Shafiq
ACM Transactions on Privacy and Security, 2017

TIST **A Traffic Flow Approach to Early Detection of Gathering Events: Comprehensive Results**
Amin Khezerlou, Xun Zhou, Lufan Li, Zubair Shafiq, Alex X. Liu, Fan Zhang
ACM Transactions on Intelligent Systems and Technology, 2017

IMC **Measuring and Mitigating OAuth Access Token Abuse by Collusion Networks**
Shehroze Farooqi, Fareed Zaffar, Nektarios Leontiadis, Zubair Shafiq
ACM Internet Measurement Conference, London, 2017
Best Paper Award
CACM Research Highlights 2020

IMC **The Ad Wars: Retrospective Measurement and Analysis of Anti-Adblock Filter Lists**
Umar Iqbal, Zubair Shafiq, Zhiyun Qian
ACM Internet Measurement Conference, London, 2017

SIGMETRICS **Characterizing and Modeling Patching Practices of Industrial Control Systems**
Brandon Wang, Xiaoye Li, Leandro P. de Aguiar, Daniel S. Menasche, Zubair Shafiq
ACM International Conference on Measurement and Modeling of Computer Systems, Urbana-Champaign, 2017

PETS **Detecting Anti Ad-blockers in the Wild**
Muhammad Haris Mughees, Zhiyun Qian, Zubair Shafiq
Privacy Enhancing Technologies Symposium, Minneapolis, 2017

ICDM **Accurate Detection of Automatically Spun Content via Stylometric Analysis**
Usman Shahid, Shehroze Farooqi, Raza Ahmad, Zubair Shafiq, Padmini Srinivasan, Fareed Zaffar
IEEE International Conference on Data Mining, New Orleans, 2017

CHI **Revisiting The American Voter on Twitter**
Huyen Le, G.R. Boynton, Yelena Mejova, Zubair Shafiq, Padmini Srinivasan
ACM Conference on Human Factors in Computing Systems, Denver, 2017

ICDCS **Distributed Load Balancing in Key-Value Networked Caches**
Sikder Huq, Zubair Shafiq, Sukumar Ghosh, Amir Khakpour, Harkeerat Bedi
IEEE International Conference on Distributed Computing Systems, Atlanta, 2017

ICNP **Peering vs. Transit: Performance Comparison of Peering and Transit Interconnections**
Adnan Ahmed, Zubair Shafiq, Harkeerat Bedi, Amir Khakpour
IEEE International Conference on Network Protocols, Toronto, 2017

ICNP **Suffering from Buffering? Detecting QoE Impairments in Live Video Streams**
Adnan Ahmed, Zubair Shafiq, Harkeerat Bedi, Amir Khakpour
IEEE International Conference on Network Protocols, Toronto, 2017

ICNP **Multipath TCP Traffic Diversion Attacks and Countermeasures**
Ali Munir, Zhiyun Qian, Zubair Shafiq, Alex Liu, Franck Le
IEEE International Conference on Network Protocols, Toronto, 2017

ICWSM **Scalable News Slant Measurement Using Twitter**
Huyen Le, Zubair Shafiq, Padmini Srinivasan
AAAI International Conference on Web and Social Media, Denver, 2017

HT **Bumps and Bruises: Mining Presidential Campaign Announcements on Twitter**
Huyen Le, G.R. Boynton, Yelena Mejova, Zubair Shafiq, Padmini Srinivasan
ACM Conference on Hypertext and Social Media, Prague, 2017

Networking **Cascade Size Prediction in Online Social Networks**
Zubair Shafiq, Alex Liu
IFIP Networking, Prague, 2017
Best Paper Award Candidate (3 nominations out of 43 accepted papers)

Networking **A Graph Theoretic Approach to Fast and Accurate Malware Detection**
Zubair Shafiq, Alex Liu
IFIP Networking, Prague, 2017

eCrime **Characterizing Key Stakeholders in an Online Black-Hat Marketplace**
Shehroze Farooqi, Muhammad Ikram, Emiliano De Cristofaro, Arik Friedman, Guillaume Jourjon, Dali Kaafar, Zubair Shafiq, Fareed Zaffar
IEEE/APWG Symposium on Electronic Crime Research, Prague, 2017

ICNP **Optimizing Internet Transit Routing for Content Delivery Networks**
Faraz Ahmed, Zubair Shafiq, Amir Khakpour, Alex Liu
IEEE International Conference on Network Protocols, Singapore, 2016

DSN **Malware Slums: Measurement and Analysis of Malware on Traffic Exchanges**
Salman Yousaf, Umar Iqbal, Shehroze Farooqi, Raza Ahmad, Zubair Shafiq, Fareed Zaffar
IEEE/IFIP International Conference on Dependable Systems and Networks, France, 2016

SIGMETRICS **QoE Analysis of a Large-Scale Live Video Streaming Event**
Adnan Ahmed, Zubair Shafiq, Amir R. Khakpour
ACM International Conference on Measurement and Modeling of Computer Systems, France, 2016

ICDCS	**The Internet is For Porn: Measurement and Analysis of Online Adult Traffic** Faraz Ahmed, Zubair Shafiq, Alex X. Liu *IEEE International Conference on Distributed Computing Systems*, Japan, 2016
INFOCOM	**Characterizing Caching Workload of a Large Commercial Content Delivery Network** Zubair Shafiq, Amir R. Khakpour, Alex X. Liu *IEEE International Conference on Computer Communications*, San Francisco, 2016
SIGSPATIAL	**A Traffic Flow Approach to Early Detection of Gathering Events** Xun Zhou, Amin Vahedian Khezerlou, Alex Liu, Zubair Shafiq, Fan Zhang *ACM International Conference on Advances in Geographic Information Systems*, San Francisco, 2016
CIKM	**The Rich and the Poor: A Markov Decision Process Approach to Optimizing Taxi Driver Revenue Efficiency** Huigui Rong, Xun Zhou, Chang Yang, Zubair Shafiq, Alex Liu *ACM International Conference on Information and Knowledge Management*, Indianapolis, 2016
TON	**Characterizing and Optimizing Cellular Network Performance during Crowded Events** Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Shobha Venkataraman, Jia Wang *IEEE/ACM Transactions on Networking*, 2016
SMP	**What Campaigns Become as Social Media Become the Infrastructure of Political Communication** G.R. Boynton, Huyen Le, Yelena Mejova, Zubair Shafiq, Padmini Srinivasan *Social Media and Politics*, 2016
TMC	**Geospatial and Temporal Dynamics of Application Usage in Cellular Data Networks** Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang *IEEE Transactions on Mobile Computing*, 2015
NSF/FCC QoE	**Tracking Mobile Video QoE in the Encrypted Internet** Zubair Shafiq *NSF/FCC Workshop on Tracking Quality of Experience in the Internet*, Princeton, 2015
NSF/FCC QoE	**Bidirectional Crosslayer QoE Optimization** Srikanth Sundaresan, Zubair Shafiq *NSF/FCC Workshop on Tracking Quality of Experience in the Internet*, Princeton, 2015
IMC	**Paying for Likes? Understanding Facebook Like Fraud Using Honeypots** Emiliano De Cristofaro, Arik Friedmam, Guillaume Jourjon, Dali Kaafar, Zubair Shafiq *ACM Internet Measurement Conference*, 2014
SIGMETRICS	**Understanding the Impact of Network Dynamics on Mobile Video User Engagement** Zubair Shafiq, Jeffrey Erman, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang *ACM International Conference on Measurement and Modeling of Computer Systems*, 2014
SIGMETRICS	**Revisiting Caching in Content Delivery Networks** Zubair Shafiq, Alex X. Liu, Amir Khakpour *ACM International Conference on Measurement and Modeling of Computer Systems*, 2014
SIGMETRICS	**A First Look at Cellular Network Performance during Crowded Events** Zubair Shafiq, Alex X. Liu, Amir Khakpour *ACM International Conference on Measurement and Modeling of Computer Systems*, 2013
ICNP	**Who are You Talking to? Breaching Privacy in Encrypted IM Networks** Muhammad U. Ilyas, Zubair Shafiq, Alex X. Liu, Hayder Radha *IEEE International Conference on Network Protocols*, 2013

CSCW **Is News Sharing on Twitter Ideologically Biased?**
Jonathan Morgan, Cliff Lampe, Zubair Shafiq
ACM Conference on Computer Supported Cooperative Work and Social Computing, 2013

ACM HotNets **Cross-Path Inference Attacks on Multipath TCP**
Zubair Shafiq, Franck Le, Mudhakar Srivatsa, Alex X. Liu
ACM Workshop on Hot Topics in Networks, 2013

TON **Large Scale Measurement and Characterization of Cellular Machine-to-Machine Traffic**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
IEEE/ACM Transactions on Networking, 2013

JSAC **Identifying Leaders and Followers in Online Social Networks**
Zubair Shafiq, Muhammad U. Ilyas, Alex X. Liu, Hayder Radha
IEEE Journal on Selected Areas in Communications, 2013

JSAC **A Distributed Algorithm for Identifying Information Hubs in Social Networks**
Muhammad U. Ilyas, Zubair Shafiq, Alex X. Liu, Hayder Radha
IEEE Journal on Selected Areas in Communications, 2013

JNSM **TCAMChecker: A Software Approach to the Error Detection and Correction of TCAM-based Networking Systems**
Zubair Shafiq, Chad Meiners, Alex Liu, Ke Shen, Zheng Qin
Springer Journal of Network and Systems Management, 2012

ICNP **A Semantics Aware Approach to Automated Reverse Engineering Unknown Protocols**
Yipeng Wang, Xiaochun Yun, Zubair Shafiq, Alex X. Liu, Zhibin Zhang, Liyan Wang, Danfeng (Daphne) Yao, Yongzheng Zhang, Li Guo
IEEE International Conference on Network Protocols, 2012
Best Paper Award

SIGMETRICS **A First Look at Cellular Machine-to-Machine Traffic – Large Scale Measurement and Characterization**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
ACM International Conference on Measurement and Modeling of Computer Systems, London, 2012

ICSE **A Large Scale Exploratory Analysis of Software Vulnerability Life Cycles**
Muhammad Shahzad, Zubair Shafiq, Alex X. Liu
International Conference on Software Engineering, Switzerland, 2012

INFOCOM **Characterizing Geospatial Dynamics of Application Usage in a 3G Cellular Data Network**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Jia Wang
IEEE Conference on Computer Communications, Orlando, 2012

SIGMETRICS **Characterizing and Modeling Internet Traffic Dynamics of Cellular Devices**
Zubair Shafiq, Lusheng Ji, Alex X. Liu, Jia Wang
ACM International Conference on Measurement and Modeling of Computer Systems, San Jose, 2011

Networking **A Random Walk Approach to Modeling the Dynamics of the Blogosphere**
Zubair Shafiq, Alex X. Liu
IFIP Networking, Spain, 2011

INFOCOM **A Distributed and Privacy-Preserving Algorithm for Identifying Information Hubs in Social Networks**
Muhammad U. Ilyas, Zubair Shafiq, Alex X. Liu, Hayder Radha
IEEE Conference on Computer Communications, Spain, 2011

RAID **PE-Miner: Mining Structural Information to Detect Malicious Executables in Realtime**
Zubair Shafiq, Syeda Momina Tabish, Fauzan Mirza, Muddassar Farooq
International Symposium On Recent Advances In Intrusion Detection, France, 2009

GECCO **Evolvable Malware**
Sadia Noreen, Shafaq Murtaza, Zubair Shafiq, Muddassar Farooq
ACM Genetic and Evolutionary Computation Conference, Canada, 2009

CCS AISec **Using Spatio-Temporal Information in API Calls with Machine Learning Algorithms for Malware Detection and Analysis**
Faraz Ahmed, Haider Hameed, Zubair Shafiq, Muddassar Farooq
Workshop on Security and Artificial Intelligence, ACM Conference on Computer & Communications Security, Chicago, 2009

KDD CSI **Malware Detection using Statistical Analysis of Byte-Level File Content**
Syeda Momina Tabish, Zubair Shafiq, Muddassar Farooq
Workshop on CyberSecurity and Intelligence Informatics (CSI), ACM Conference on Knowledge Discovery and Data Mining, France, 2009

VB **PE-Probe: leveraging packer detection and structural information to detect malicious portable executables**
Zubair Shafiq, Syeda Momina Tabish, Muddassar Farooq
Virus Bulletin, Switzerland, 2009

Elsevier **Fuzzy Case Based Reasoning for Facial Expression Recognition**
Aasia Khanum, Muid Mufti, M. Y. Javed, Zubair Shafiq
Elsevier Fuzzy Sets and Systems, 2009

EvoComNet **A Comparative Study of Fuzzy Inference Systems, Neural Networks and Adaptive Neuro Fuzzy Inference Systems for Portscan Detection**
Zubair Shafiq, Muddassar Farooq, Syed Ali Khayam
Applications of Evolutionary Computing, EvoComNet, Italy, 2008

DIMVA **Embedded Malware Detection using Markov n-grams**
Zubair Shafiq, Syed Ali Khayam, Muddassar Farooq
International Conference on Detection of Intrusions, Malware and Vulnerability Assessment, France, 2008

GECCO **Improving Accuracy of Immune Inspired Malware Detectors using Intelligent Features**
Zubair Shafiq, Syed Ali Khayam, Muddassar Farooq
ACM Genetic and Evolutionary Computation Conference, Atlanta, 2008

Funding

External Competitive Research Grants

UC **Auditing Compliance of Data Privacy Laws in California**
UC Partnerships in Computational Transformation
PI, Duration: 2022-2023, Total: $160,000, Share: $80,000
Personnel: Zubair Shafiq (PI: UC Davis); Athina Markopoulou (PI: UC Irvine); Gene Tsudik (Co-PI: UC Irvine)

NSF-SaTC **Defending against Emerging Stateless Web Tracking**
National Science Foundation
PI, Duration: 2022-2026, Total: $1,200,000, Share: $400,000
Personnel: Zubair Shafiq (PI: UC Davis); Alexandros Kapravelos (PI: NC State); Anupam Das (Co-PI: NC State)

CITRIS and **Auditing the compliance of California consumer privacy regulations at scale**
the Banatao Center for Information Technology Research in the Interest of Society (CITRIS)
Institute Co-PI, Duration: 2021-2022, Total: $60,000, Share: $20,000
Personnel: Serge Egelman (Co-PI: UC Berkeley); Zubair Shafiq (Co-PI: UC Davis)

NSF-SaTC- **Protecting Personal Data Flow on the Internet**
Frontier National Science Foundation
PI, Duration: 2020-2025, Total: $10,000,000, Share: $1,100,000
Personnel: Zubair Shafiq (PI: UC Davis); Athina Markopoulou (PI: UC Irvine); Konstantinos Psounis (PI: USC); David Choffnes (PI: Northeastern)

NSF-CAREER **Quality of Experience and Network Management in the Encrypted Internet**
National Science Foundation
PI, Duration: 2018-2023, Total: $500,000, Share: $500,000
Personnel: Zubair Shafiq (PI: UC Davis)

NSF-SaTC **A Multi-Layer Learning Approach to Mobile Traffic Filtering**
National Science Foundation
PI, Duration: 2018-2021, Total: $500,000, Share: $250,000
Personnel: Zubair Shafiq (PI: UC Davis); Athina Markopoulou (PI: UC Irvine)

NSF-SaTC **The Web Ad Technology Arms Race: Measurement, Analysis, and Countermeasures**
National Science Foundation
PI, Duration: 2017-2020, Total: $500,000 + $16,000 (REU Supplement 2019) + $16,000 (REU Supplement 2021), Share: $282,000
Personnel: Zubair Shafiq (PI: UC Davis); Zhiyun Qian (PI: UC Riverside)

NSF-NeTS **Towards Scalable and Energy Efficient Cellular IoT Communication**
National Science Foundation
PI, Duration: 2016-2019, Total: $500,000, Share: $166,000
Personnel: Zubair Shafiq (PI: Iowa); K.K. Ramakrishnan (PI: UC Riverside); Koushik Kar (PI: RPI)

NSF-SaTC **Multipath TCP Side Channel Vulnerabilities and Defenses**
National Science Foundation
PI, Duration: 2015-2018, Total: $500,000, Share: $167,000
Personnel: Zubair Shafiq (PI: Iowa); Zhiyun Qian (PI: UC Riverside); Alex Liu (PI: Michigan State University)

NSF-NeTS **Towards Measurement and Optimization of Internet Video Quality of Experience**
National Science Foundation
PI, Duration: 2015-2018, Total: $175,000 + $16,000 (REU Supplement 2016), Share: $191,000
Personnel: Zubair Shafiq (PI: Iowa)

DTL **Detection and Circumvention of Ad-Block Detectors**
Data Transparency Lab
PI, Duration: 2016-2017, Total: $56,000, Share: $28,000
Personnel: Zubair Shafiq (PI: Iowa); Zhiyun Qian (PI: UC Riverside)

Internal Competitive Research Grants

Academic Senate	**Socio-Computational Interventions to Mitigate Misinformation in Recommendations** Noyce Foundation PI, Duration: 2022-2023, Total: $25,000 Personnel: Magdalena Wojcieszak (PI), Zubair Shafiq (Co-PI)
Noyce	**Measuring and Mitigating Biases in Social Recommendation Algorithms** Noyce Foundation PI, Duration: 2022-2023, Total: $236,000 Personnel: Zubair Shafiq (PI), Magdalena Wojcieszak (Co-PI)
Noyce	**Cross-Layer Approach to Enhance Security/Privacy of AI-enabled IoT Eco-Systems** Noyce Foundation Co-PI, Duration: 2022-2023, Total: $225,000 Personnel: Chen-Nee Chuah (PI), Zubair Shafiq (Co-PI), Houman Homayoun (Co-PI)
Noyce	**Measuring and Mitigating Biases in Social Recommendation Algorithms** Noyce Foundation PI, Duration: 2021-2022, Total: $235,690 Personnel: Zubair Shafiq (PI), Xin Liu (Co-PI), Magdalena Wojcieszak (Co-PI)
Noyce	**Cross-Layer Approach to Enhance Security/Privacy of AI-enabled IoT Eco-Systems** Noyce Foundation Co-PI, Duration: 2021-2022, Total: $225,000 Personnel: Chen-Nee Chuah (PI), Zubair Shafiq (Co-PI), Houman Homayoun (Co-PI)
UIRF	**Social Media Powered Real-Time Digital News Recommendation** University of Iowa Research Foundation PI, Duration: 2015-2016, Total: $75,000 Personnel: Zubair Shafiq (PI)
Obermann	**Heterogeneous Network Data Analytics to Improve Urban Sustainability** Obermann Center Interdisciplinary Research Grant PI, Duration: 2015-2016, Total: $12,000 Personnel: Xun Zhou (PI); Zubair Shafiq (Co-PI)

Industry Grants and Unrestricted Gifts

Siemens	PI, Duration: 2021, Total: $60,000, Share: $60,000 Personnel: Zubair Shafiq (PI: UC Davis)
Siemens	PI, Duration: 2019, Total: $30,000, Share: $30,000 Personnel: Zubair Shafiq (PI: Iowa)
Siemens	PI, Duration: 2018, Total: $60,000, Share: $60,000 Personnel: Zubair Shafiq (PI: Iowa)
Verizon	PI, Duration: 2018, Total: $20,000, Share: $20,000 Personnel: Zubair Shafiq (PI: Iowa)
Minim	PI, Duration: 2018, Total: $66,164, Share: $66,164 Personnel: Zubair Shafiq (PI: Iowa)
Siemens	PI, Duration: 2017, Total: $30,000, Share: $30,000 Personnel: Zubair Shafiq (PI: Iowa)
Nokia	PI, Duration: 2017, Total: $53,200, Share: $53,200 Personnel: Zubair Shafiq (PI: Iowa)
Futurewei	PI, Duration: 2017, Total: $100,384, Share: $100,384 Personnel: Zubair Shafiq (PI: Iowa)

Facebook   PI, Duration: 2016, Total: $8,400, Share: $8,400
Personnel: Zubair Shafiq (PI: Iowa)

Teaching

ECS 289M   **Topics in Privacy**
Spring 2024, University of California at Davis

ECS 188   **Ethics in an Age of Technology**
Winter 2024, University of California at Davis

ECS 152A   **Computer Networks**
Fall 2023, University of California at Davis

FYS   **Big Data, Big Brother**
Winter 2023, University of California at Davis

ECS 289M   **Network Security & Privacy**
Winter 2023, University of California at Davis

ECS 152A   **Computer Networks**
Fall 2022, University of California at Davis

ECS 152A   **Computer Networks**
Spring 2022, University of California at Davis

ECS 153   **Computer Security**
Winter 2022, University of California at Davis

ECS 289M   **Data-Driven Security**
Spring 2021, University of California at Davis

ECS 152B   **Computer Networks**
Winter 2021, University of California at Davis

CS 2620   **Networking & Security for Informatics**
Spring 2020, The University of Iowa

CS 4980   **Online Advertising & Tracking**
Fall 2019, The University of Iowa

CS 2620   **Networking & Security for Informatics**
Spring 2019, The University of Iowa

CS 4980   **Internet Measurement**
Fall 2018, The University of Iowa

CS 2620   **Networking & Security for Informatics**
Spring 2018, The University of Iowa

CS 2620   **Networking & Security for Informatics**
Spring 2017, The University of Iowa

CS 4980   **Network Security and Privacy**
Fall 2016, The University of Iowa

CS 2620   **Networking & Security for Informatics**
Spring 2016, The University of Iowa

CS 4980   **Advanced Computer Networks**
Fall 2015, The University of Iowa

CS 2620 **Networking & Security for Informatics**
Spring 2015, The University of Iowa

CS 4980 **Internet Measurement**
Fall 2014, The University of Iowa

Students

Doctorate

2022-current   Rajvardhan Oak

2021-current   Pouneh Nikkhah Bahrami

2021-current   Shaoor Munir

2021-current   Yash Vekaria

2016-2021   Dr. Umar Iqbal; First Position: CIFellow/Postdoc, University of Washington

2015-2021   Dr. Shehroze Farooqi; First Position: Researcher, Palo Alto Networks

2015-2019   Dr. Huyen Le; First Position: Postdoc, National Center for Toxicological Research

Select Recent Masters Mentees

2021   Mohammad Ismail Daud

2021   Sunshine Chong

2021   Rachit Dhamija

2020   Pouneh Nikkhah Bahrami

Select Recent Undergraduate Mentees

2023   Divya Raj

2023   Shuaib Ahmed

2023   Ryan Swift

2023   Tangbaihe Wang

2023   Patrick Lee

2022   Jake Smith

2022   Christina Phan

2022   Kev Rockwell

2020-2022   Kajal Patel (NSF REU)

2020-2022   Wanyue Zhai (graduate student at Stanford)

2020-2022   Ray Ngan (NSF REU) (industry: Palo Alto Networks)

2020-2021   Surya Konkimalla

2020-2021   Charles Nguyen (industry: Apple)

2019-2021   Charlie Wolfe (NSF REU) (industry: Apple)

2021   Caelan MacArthur (NSF DREU)

2020-2021   Taimur Kashif (NSF REU) (industry: VMWare)

2019-2020   Ashton Woiwood (NSF REU)

2017   Treyton Krupp (NSF REU)

2015   Mirza Besic

High School

2023   Reeva Rao

2023	Jayalakshmi Raffill
2019	Kathy Zhong
2018	Alice Martynova
2017	William Kim
2016	Brandon Wang

External Service

Conference TPC/Reviewer	IEEE S&P (2022), PETS (2021, 2020, 2019, 2018, 2017), ACM IMC (2021, 2020), ACM CoNEXT (2019), ACM SIGMETRICS (2023, 2022, 2020, 2013), WWW (2020, 2018), ACM CSCW (2018, 2019), IEEE/IFIP TMA (2020, 2019), NDSS MADWeb Workshop (2019), IEEE INFOCOM (2017, 2015, 2010, 2009), ACM WPES (2018), IEEE S&P Consumer Protection Workshop (2021, 2020), ACM SIGCOMM Internet-QoE Workshop (2017), ACM SIGCOMM Workshop on IoT Security and Privacy (2018), WWW CyberSafety Workshop (2018), WWW Workshop on Location and the Web (2018), IEEE ICNP (2014, 2013), MASCOTS (2013), ICDCN (2017, 2018)
Journal Reviewer	IEEE/ACM Transactions on Networking, ACM Transactions on the Web, IEEE Transactions on Mobile Computing, IEEE Transactions on Network and Service Management, ACM Transactions on Multimedia Computing, IEEE Transactions on Cognitive Communications and Networking, ACM SIGCOMM Computer Communication Review, Elsevier Computer Communications, Elsevier Performance Evaluation, Springer Wireless Networks
PC Co-Chair	Privacy Enhancing Technologies Symposium (PETs), 2025
PC Co-Chair	Privacy Enhancing Technologies Symposium (PETs), 2024
PC Co-Chair	Workshop on Technology and Consumer Protection (ConPro'23), IEEE Symposium on Security & Privacy ("Oakland")
PC Co-Chair	Workshop on Technology and Consumer Protection (ConPro'22), IEEE Symposium on Security & Privacy ("Oakland")
PC Co-Chair	Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb'23), Network and Distributed System Security Symposium (NDSS)
PC Co-Chair	Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb'22), Network and Distributed System Security Symposium (NDSS)
Publicity Co-Chair	ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT 2020)
Co-Chair	NSF NeTS Early Career Investigators Workshop 2019
PC Co-Chair	Student Workshop - ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT 2018)
PC Co-Chair	WWW 8th International Workshop on Location and the Web (LocWeb 2018)
Poster Chair	ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS 2018)
Technical Committee	Elsevier Computer Communications (2015-2019)
Guest Editor	Special Issue on Mobile Traffic Analytics, Elsevier Computer Communications (2016)
Editorial Board	Proceedings on Privacy Enhancing Technologies (PoPETs) (2019, 2020, 2021)

Panelist	NSF (2017, 2018, 2019, 2020, 2021, 2022, 2023)

Internal Service

Chair	Departmental Colloquium Series Department of Computer Science, University of California Davis, 2021-
Member	Diversity, Equity, Inclusion Committee College of Engineering, University of California Davis, 2021-2022
Committee	Departmental Graduate Committee Department of Computer Science, University of Iowa, 2019-2020
Chair	Departmental Colloquium Series Department of Computer Science, University of Iowa, 2019-2020
Member	Executive Committee, Iowa Initiative for Artificial Intelligence (IIAI) The University of Iowa, 2019-2020
Member	Department Executive Committee Department of Computer Science, The University of Iowa, 2016-2019
Member	Faculty Recruitment Committee Department of Computer Science, The University of Iowa, 2015-2020
Mentor	Black Girls Do Science College of Engineering, The University of Iowa, 2015-2016
Mentor	Iowa Edge Classroom Experience Center for Diversity and Enrichment, The University of Iowa, 2015-2018
Mentor	Summer Research Opportunities Program (SROP) Graduate College, The University of Iowa, 2017
Mentor	Secondary Student Training Program (SSTP) Belin-Blank Center, The University of Iowa, 2016-2019

Patents

USPTO 10484881	Jia Wang, Lusheng Ji, Alex X. Liu, Zubair Shafiq. Optimization of cellular network architecture based on device type-specific traffic dynamics. November 2019
USPTO 10420167	Jia Wang, Lusheng Ji, Alex X. Liu, Jeffrey Pang, Zubair Shafiq. Cellular Connection Sharing. September 2019

Expert Testimony & Reports (in the past five years)

4:20-cv-05146	**Calhoun v. Google**
4:21-cv-02155	**In re Google RTB Consumer Privacy Litigation**
5:23-cv-02431	**Doe v. Google**
22-01-88230-D	**State of Texas v. Google**
A 2002633	**Doe v. Bon Secours Mercy Health**

24-C-20-000591	**Doe v. Medstar Health**
19-2-26674-1	**Doe v. Virginia Mason**
23CV037304	**Doe v. Family Planning Associates Medical Group**
22-cv-03580	**In re Meta Pixel Healthcare Litigation**
23OT01-0026	**Stake v. Knox**
23-cv-00964	**Griffith v. TikTok**
22STCV36304	**Doe v. Adventist**
3:22-cv-07465	**Hazel v. Prudential**

Litigation Consulting (in the past five years)

Bleichmar Fonti & Auld

Simmons Hanly Conroy

Lieff Cabraser Heimann & Bernstein

DiCello Levitt Gutzler

Norton Rose Fulbright

Pritzker Levine

Social Media Victims Law Center

Girard Sharp

Hammond Law

Caddell & Chapman

Whatley Kallas

Office of the Attorney General, Texas

AZA Law

Susman Godfrey

APPENDIX B: MATERIALS CONSIDERED

- Prudential's Responses to Requests for Admission (set one)
- Defendants' Responses to Interrogatories (sets one and two)
- Renz Deposition Transcript
- Rafferty Deposition Transcript
- Bao Deposition Transcript
- AP0000007
- AP0000039
- AP0000167
- AP0000169
- AP0000239
- AP0000388
- AP0000392
- AP0000394
- AP0000395
- AP0000483
- AP0000490
- AP0000492
- AP0000493
- AP0000494
- AP0000505
- AP0000506
- AP0000507
- AP0000509
- AP0000511
- AP0000512
- AP0000513
- AP0000514
- AP0000515
- AP0000516
- AP0000517
- AP0000518
- AP0000519

- AP0000577
- AP0000585
- AP0000610
- AP0000632
- AP0000712
- AP0000743
- AP0000768
- AP0000772
- AP0000847
- AP0000858
- AP0000865
- AP0000866
- AP0000867
- AP0000868
- AP0000869
- AP0000870
- AP0000872
- AP0000874
- AP0000876
- AP0000885
- AP0000887
- AP0000889
- AP0000896
- AP0000898
- AP0000900
- AP0000903
- AP0000905
- AP0000907
- AP0000908
- AP0000909
- AP0000910
- AP0000911
- AP0000912

- AP0000913
- AP0000914
- AP0000915
- AP0000916
- AP0000917
- AP0000918
- AP0000919
- AP0000920
- AP0000921
- AP0000922
- PRU0000086
- PRU0000088
- PRU0000089
- PRU0000090
- PRU0000091
- PRU0000092
- PRU0000093
- PRU0000094
- PRU0000095
- PRU0000096
- PRU0000097
- PRU0002712
- PRU0002714
- ActiveProspect Highly Confidential Source Code documents produced for inspection
- term.prudential.com
  - term.prudential.com.har (accessed November 2023)
  - Internet Archive's Wayback Machine, (https://web.archive.org/web/20210401000000*/https://term.prudential.com/life)
  - Screen Recording.mov
- Translate TrustedForm Python Script
  - Translated Snapshot Payload
  - Translated Events Payload
- Amjad, A.H., Shafiq, Z. and Gulzar, M.A., 2023, January. *Blocking JavaScript without Breaking the Web*. In Privacy Enhancing Technologies Symposium (PETS).

- Acar, G., Englehardt, S. and Narayanan, A., 2020. *No boundaries: data exfiltration by third parties embedded on web pages*. Proceedings on Privacy Enhancing Technologies.

- Senol, A., Acar, G., Humbert, M. and Borgesius, F.Z., 2022. *Leaky forms: A study of email and password exfiltration before form submission*. In 31st USENIX Security Symposium (USENIX Security 22) (pp. 1813-1830).

- bootstrap.js (https://cdn.trustedform.com/bootstrap.js?provide_referrer=false&field=xxTrustedFormCertUrl&l=17013362437130.2550676600214141&invert_field_sensitivity=false)

- trustedform-1.9.4.js (https://cdn.trustedform.com/trustedform-1.9.4.js)

- https://activeprospect.com/resources/discovering-trustedform-api/

- https://cdn.assurance.com/insurance/public/assets/trustedForm-4a1205758bed9df95ef0ff78d02f73edd84361c32de02c6addd014f63fde670a.js

- https://almanac.httparchive.org/en/2022/javascript

- https://cloud.google.com/security/products/recaptcha?hl=en

- https://developer.mozilla.org/en-US/docs/Glossary/Cookie

- https://developer.mozilla.org/en-US/docs/Glossary/Cryptographic_hash_function

- https://developer.mozilla.org/en-US/docs/Web/API/Document_Object_Model

- https://developer.mozilla.org/en-US/docs/Web/API/Document/scroll_event

- https://developer.mozilla.org/en-US/docs/Web/API/Element/click_event

- https://developer.mozilla.org/en-US/docs/Web/API/Element/keydown_event

- https://developer.mozilla.org/en-US/docs/Web/API/Event

- https://developer.mozilla.org/en-US/docs/Web/API/EventTarget/addEventListener.

- https://developer.mozilla.org/en-US/docs/Web/API/EventTarget/addEventListener#browser_compatibility

- https://developer.mozilla.org/en-US/docs/Web/API/MutationObserver

- https://developer.mozilla.org/en-US/docs/Web/API/MutationObserver#browser_compatibility

- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cookie

- https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/POST

- https://developers.activeprospect.com/docs/trustedform/getting-started/

- https://docs.house.gov/meetings/IF/IF17/20180614/108413/HHRG-115-IF17-20180614-SD007.pdf

- https://gs.statcounter.com/browser-market-share/all/chart.php?device=Desktop%20%26%20Mobile%20%26%20Tablet%20%26%20Console&device_hidden=desktop%2Bmobile%2Btablet%2Bconsole&multi-device=true&statType_hidden=browser&region_hidden=US&granularity=monthly&statType=Browser&region=United%20States%20of%20America&fromInt=202304&toInt=202404&fromMonthYear=2023-04&toMonthYear=2024-04&csv=1

- https://innovation.ox.ac.uk/incubator-ventures/oxford-bio-chronometrics/

- https://oxford-biochron.com/
- https://trends.builtwith.com/analytics/Oxford-Biochronometrics
- https://trends.builtwith.com/widgets/reCAPTCHA
- https://webkit.org/tracking-prevention/#intelligent-tracking-prevention-itp
- https://www.cloudflare.com/learning/bots/what-is-a-bot/
- https://www.computerhope.com/issues/ch000891.htm
- https://www.google.com/recaptcha/about/
- https://www.google.com/recaptcha/intro/?zbcode=inc5000